

REMARKS

Claims 1-50 are pending in this application, all of which have been rejected. In view of the above amendments and following remarks, Applicants respectfully request reconsideration of the application.

Amendments to the Claims

Applicants have amended claims, in part, to change dependencies, for readability, and correct grammar. Specifically, the dependencies of dependent claims 19, 26, 27, 29, 33, 34, 39, and 42 have been changed. No new matter is added by way of these amendments.

Rejections under 35 U.S.C. §112

In paragraphs 3 and 4, claims 15-16 have been rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Specifically, the Examiner contends that claim 15 contains the trademark "Microsoft Office" and "Microsoft Windows" as a limitation to identify a product. In response, Applicants have amended claim 15 to read "wherein the application is provided in a *Microsoft Office product* and the operating system is *Microsoft Windows operating system.*" (emphasis added). As such, the trademark terms are not in themselves the product. Applicants therefore request that the Examiner withdraw the 35 U.S.C. §112, second paragraph, rejections of claims 15-16.

Rejections under 35 U.S.C. §101

In paragraphs 5 and 6, the Examiner rejected claims 1-39 under 35 U.S.C. §101 because the claimed information is directed to non-statutory subject matter. Specifically, the Examiner contends that claims 1-39 "recite of software alone and of itself that is not tangibly embodied." In response, independent claims 1, 11, and 20 have been amended to recite a "computer implemented method." Additionally,

independent claims 24 and 31 have been amended to recite a “software product stored on a computer readable medium.” As such, Applicants request that the rejections under 35 U.S.C. §101 be withdrawn.

Rejections under 35 U.S.C. §102

In paragraphs 7 and 8, the Examiner rejected claims 1-50 under 35 U.S.C. §102(e) as being anticipated by *England* (USPN 6,775,779). Applicants respectfully traverse.

Claims 1-10 and claims 24-30

As per independent claim 1, the Examiner finds all elements to be taught by *England* et al., and cite col. 2, line 66 through col. 3, line 13 and col. 9, line 55 through col. 10, line 5 for support.

Claim 1 recites in part “determining...whether *the file being accessed is secured*” and “when the file is determined to be secured, activating a cipher module and loading the file through the cipher module into the application” (emphasis added). Therefore, embodiments of the present invention determine if files, not applications or modules that operate on the files, are secured. If the files are secured, then a cipher module is utilized to operate on the secured file. The secured files, in exemplary embodiments, are files that may be partly encrypted and may contain access rules which define access privileges.

In contrast, the cited portions of *England* refer to “running designated processes, libraries, or other software components at a higher level of protection” (col. 2, line 64 – col. 3, line 1). *England* describes as examples, “rights-management operation-system modules, communication drivers, and video decoding applications programs” which can run in protected memory that is not accessible by other modules (col. 3, line 3-6). Thus, *England* is concerned with protecting applications, “where the application must be protected from viruses or other malicious code” (col. 3, line 26-27).

England does discuss having trusted modules that exchange data among themselves, whereby trusted modules can identify other trusted modules (col. 3, line 9-17). These modules, however, are defined as “packages of executable instructions and data which may perform functions for OSs or for applications” (col. 5, line 25-26). Thus, *England* is directed to utilizing a protected memory to run trusted modules and protected applications.

England does not contemplate determining whether the file being accessed is secured. Because secured files are not taught, *England* further cannot contemplate the user of a cipher module in connection with the secured files. In fact, files, secured or not, are not even discussed in *England*. Therefore, claim 1 is not anticipated by *England*. Further, claims 2-10 which depend from claim 1 are not anticipated by *England* for the same reasons as claim 1.

Claim 24 is rejected by the Examiner for the same reasons as claim 1. Claim 24 recites in part “when the file is determined to be secured, activating a cipher module that operates in the operating system; loading the file through the cipher module into the application.” As discussed above, *England* does not contemplate the use of secured files or the cipher module in connection with the secured files. Therefore, claim 24 is not anticipated by *England*. Additionally, claims 25-30, which depend from claim 24, are not anticipated for the same reasons as claim 24.

Claims 11-19

With regard to independent claim 11, the Examiner cites to the same section of *England* for support as that of claim 1. Claim 11 recites in part “encrypting the file with the file key in a cipher module to produce an encrypted portion” and “preparing security information for the encrypted portion, the security information being encrypted and including the file key and access rules to control access to the encrypted portion” of the file.

As previously, discussed, the cited portions of *England* (along with the rest of the patent) refer to protecting applications and modules from viruses and other malicious code. *England* does not contemplate the protection of the files, themselves. In fact, there is no reference in *England* to encrypting files with a file key and preparing security information for the encrypted portion.” If the Examiner maintains this rejection, Applicants request that the Examiner point out specifically where *England* discusses encrypting the file and preparing security information for the encrypted portion.

Therefore, claim 11 is not anticipated by *England*. Claims 12-19, which depend from claim 11, are also not anticipated by *England* for the same reasons as for claim 11.

Claims 20-23

With respect to independent claim 20, the Examiner once again cites to the same section of *England* for support as that of claim 1. Claim 20, however, recites in part “determin[ing] whether the file being accessed is secured.”

As previously discussed, *England* does not contemplate the use of secured files. Therefore, *England* cannot disclose determining whether the file being accessed is secured. As such, independent claim 20 is not anticipated by *England*. Additionally, claims 21-23 are also not anticipated by *England* by way of their dependency from claim 20.

Claims 31-39

With respect to independent claim 31, the Examiner also cites to the same section of *England* for support as that of claim 1. Independent claim 31, however, recites in part “encrypting the file with the file key in a cipher module to produce an encrypted file” and “storing, in a storage space, a secured file including the encrypted file and a header.”

Because *England* does not contemplate having secured files, *England* cannot teach or suggest encrypting the file with the file key or storing a secured file including the encrypted file and a header. Therefore, independent claim 31 is not anticipated by *England*. Further, claims 32-39, which depend from claim 31, are not anticipated by *England* for the same reasons as that of claim 31.

Claims 40-50

In regards to independent claim 40, the Examiner cited to the previously cited portions of *England* along with col. 6, line 33-45. As previously discussed, col. 2, line 66 through col. 3, line 13 and col. 9, line 55 through col. 10, line 5 of *England* refer to the protection and utilization of applications and modules. Col. 6, line 33-45 merely teaches an access-control table which contains bits that determine rights for a program combination that accesses a page. For example, one bit of each entry indicates whether *the programs specified have read, write, or execution privileges* for the page specified. Once again, the cited portion only refers to program protection and access, not file protection and access, as contemplated by embodiments of the present invention.

Claim 40 recites in part "accessing the file that includes security information and an encrypted portion, the security information further including a file key and access rules, and the encrypted portion being an encrypted version of the file" and "a cipher module activating upon determining that the file being accessed is secured." Because *England* does not contemplate having secured files that include security information and an encrypted portion nor does *England* teach a cipher module activating upon determining that the file being accessed is secured, *England* does not anticipate claim 40. Further, claims 41-50, which depend from claim 40 are not anticipated by *England* for the same reasons as that of claim 40.

Conclusion

Based on the above amendments and remarks, Applicants believe that the rejections in the Office Action of October 6, 2005 are fully overcome, and that the application is in condition for allowance. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicant's undersigned representative at the number given below.

Respectfully submitted,

Chang-Ping Lee et al.

Date: 4/6/06

By: 

Susan Yee, Reg. No. 41,388

Carr & Ferrell *LLP*

2200 Geng Road

Palo Alto, CA 94303

TEL: (650) 812-3465

FAX: (650) 812-3444